



CVE-2007-0443

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2007-0443
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-04-24 16:19:00 UTC
Updated	2018-10-16 16:32:00 UTC
Description	Multiple buffer overflows in the CDDDBControl ActiveX control in Gracenote CDDDB before 20070418 allow remote attackers

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gracenote	Cddbcontrol Activex Control	All	All	All	All
Application	Gracenote	Cddbcontrol Activex Control	All	All	All	All

References

Reference
34327
SecurityTracker.com Archives - Gracenote CDDDBControl ActiveX Control Buffer Overflow in Processing Proxy Control Parameters Permits Re
GraceNote CDDDBControl Multiple Parameters ActiveX Control Buffer Overflow Vulnerability
Gracenote CDDDBControl ActiveX Buffer Overflow Vulnerability - Advisories - Secunia
IBM X-Force Exchange
Page not found - Gracenote
ZDI-07-021
SecurityFocus
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)